CNST NanoFab Facility User Computer Security and Usage Policy

This document contains policies specific to NanoFab facility computer systems, and should be considered a supplement to official NIST Information Technology Security Policies. It does not supersede those documents, although important information will be duplicated for emphasis. All NIST-wide computer policies apply to our computer systems in addition to those outlined in this document.

This security policy defines a set of controls commensurate with the risks to which our computers are exposed. The best defense for our system is a set of commonsense rules which, when adhered to, will protect our computers without becoming burdensome.

These policies are in effect during all hours.

Usage of System

- Usage of NIST machines is a privilege, not a right. Please remember these machines are property of the United States Government.
- All users of our systems and services must be authorized by the system administrators on approval by the NanoFab Manager and NanoFab Facility User Office.
- Individual users are responsible for their actions. Their responsibility exists regardless of the security mechanisms that are in place. Breaking into accounts, i.e., accessing another users account or files without permission or bypassing security is not permitted.
- Non-NIST employees, such as Facility Users, are subject to the same computer security policies as NIST employees.
- All computer system privileges will be terminated when a project has expired or finished (whichever comes first).
- Users do not have administrative rights on their PC's and cannot install applications. .
- Users should log off all workstations when they are done so that others may use them. If an account is left logged on and unattended for more than 30 minutes on one of these computers, the user may be logged off by the system administrators.
- The system administrators cannot and will not save any work before logging off users.

Physical Security

- All computers are set up to automatically lock with a password protected screensaver after 15 minutes of inactivity and will remain this way.
- Users must report any damage or loss of hardware, software, or data immediately to NanoFab staff members.
- Any suspicious behavior should be reported to the NanoFab Facility User Office immediately.

Password security

- Passwords cannot be shared. This means that there must be just one user per user ID.
- Do not allow anyone else to know your password.
- Passwords must be at least twelve (12) characters in length.

- Passwords must contain at least one digit, at least two alphabetic characters (uppercase and lowercase), and at least one special character.
- Passwords must not be in a dictionary. This means no names, places, etc. from any language.
- Passwords cannot be a person's username forward or backwards.
- No character may be repeated more than five (5) times.
- Passwords must not be trivial, e.g. asdf, qwerty, etc.
- Good passwords contain case changes and multiple words.
- Passwords must be changed once every 90 days.
- Passwords cannot be reused.
- Passwords used for our computer systems should not be used elsewhere. Outside systems have varying levels of security and those passwords may be compromised.
- Users must immediately notify the CNST system administrators if they suspect their password has been compromised and must immediately change it.

Virus Protection

- Virus protection software is enabled on all computers and should not be disabled.
- All incoming USB flash drive must be scanned for viruses!
- USB drives can only be used on file retrieval computers.

File Storage

- All user data should be saved to the NanoFab file server.
- Do not save to the computer's hard drive. Save to home drives, mapped as Z drive.
- The file server is not intended for long term storage. Users should promptly retrieve their data. Files older than 90 days are subject to deletion.

Unacceptable Use of CNST NanoFab Information Technology Resources

The use of CNST NanoFab systems and networks in a manner which is unacceptable may subject the person(s) involved to loss of all privileges to use CNST NanoFab systems, may result in other disciplinary sanctions up to and including dismissal, or may result in criminal prosecution. Unacceptable uses of CNST NanoFab systems and networks include, but are not limited to:

- Any use of CNST NanoFab information technology resources in order to obtain access to any network or system at CNST NanoFab, or elsewhere, for which the person has not been authorized, or in a manner that knowingly violates the policies of the owner of the network or system;
- Any activity that interferes with the legitimate activities of anyone using any CNST NanoFab systems or networks, or any other network or system which may be accessed from CNST NanoFab;
- Unauthorized use of a system for which the user has authorized access, including use of privileged commands on a system by a user not authorized to use such commands and

unauthorized access to information owned by someone else. For example, no user may access the root account on a Unix system or attempt to become root on the system unless he or she is authorized to do so;
- Deliberate unauthorized destruction of CNST NanoFab data or other resources;
- Any use of CNST NanoFab information technology resources to engage in illegal or unethical activities;

- CNST NanoFab expects users to conduct themselves professionally and to refrain from using CNST NanoFab resources for activities that are offensive to coworkers or the public. Some examples include the use of CNST NanoFab IT resources that contain or promote (a) matters directed toward the success or failure of a political party, candidate for partisan political office, or partisan political group, (b) engaging in any action supportive of lobbying the Congress, (c) use of Internet sites that result in an unauthorized charge to the Government, (d) participating in prohibited activities such as discriminatory conduct, gambling, and disseminating chain letters, (e) intentional and unauthorized viewing of sexually explicit or pornographic material, (f) sending personal e-mail that might be construed by the recipient to be an official communication, (g) any activity that would bring discredit on CNST NanoFab or the Department of Commerce, (h) statements viewed as harassing others based on race, age, creed, religion, national origin, color, sex, handicap, or sexual orientation, (i) any violation of statute or regulation.

Enforcement:

Individuals involved with misuse will be subject to having all computer account access indefinitely suspended at the discretion of the NanoFab Manager and the CNST IT Staff.

I have read and agree to abide by the "CNST Computer Security and Usage Policy" dated November 17, 2010 and all other related NIST IT security policies.

_____ _____

Print Name Organization

_____ _____

Signature Date